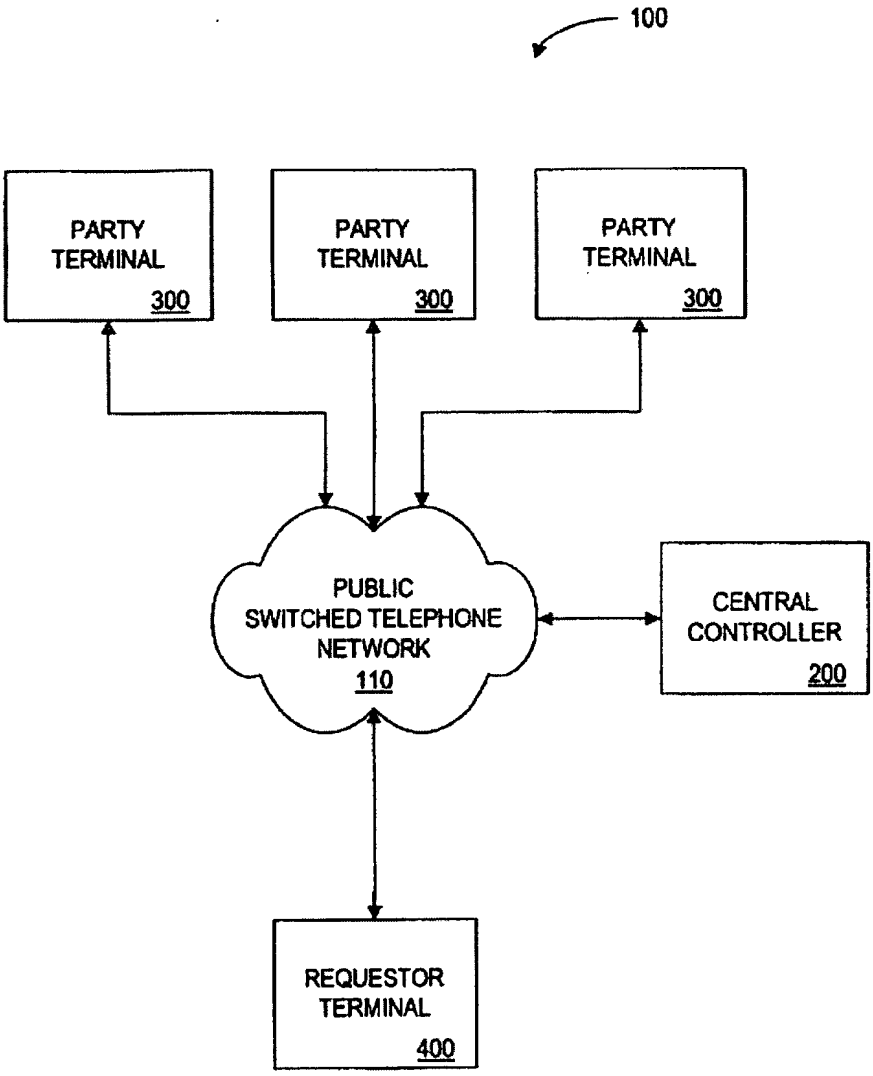
## Remarks

The paper is submitted in response to the first Office action, mailed June 30, 2005. Applicant requests a three-month extension of time to submit this response; the applicable fee is submitted herewith.

The Examiner rejected original claims 1-5 under 35 USC Section 102(b) as being anticipated by U.S. Pat. No. 5,884, 270 to Walker et al. (hereinafter "*Walker*"). Applicant respectfully traverses the rejections and requests reconsideration for the reasons set forth below. New claims 6-15 are submitted to more completely claim the invention. Minor corrections to the specification are submitted above as well. The drawings submitted with the application on October 30, 2001 were accepted by the Examiner.

*Walker* discloses techniques for anonymous communications by providing a "go between" communication service that keeps the identities of users of remote terminals ("party terminals") separate from employers who access a "requestor terminal" to fill an employment opening.

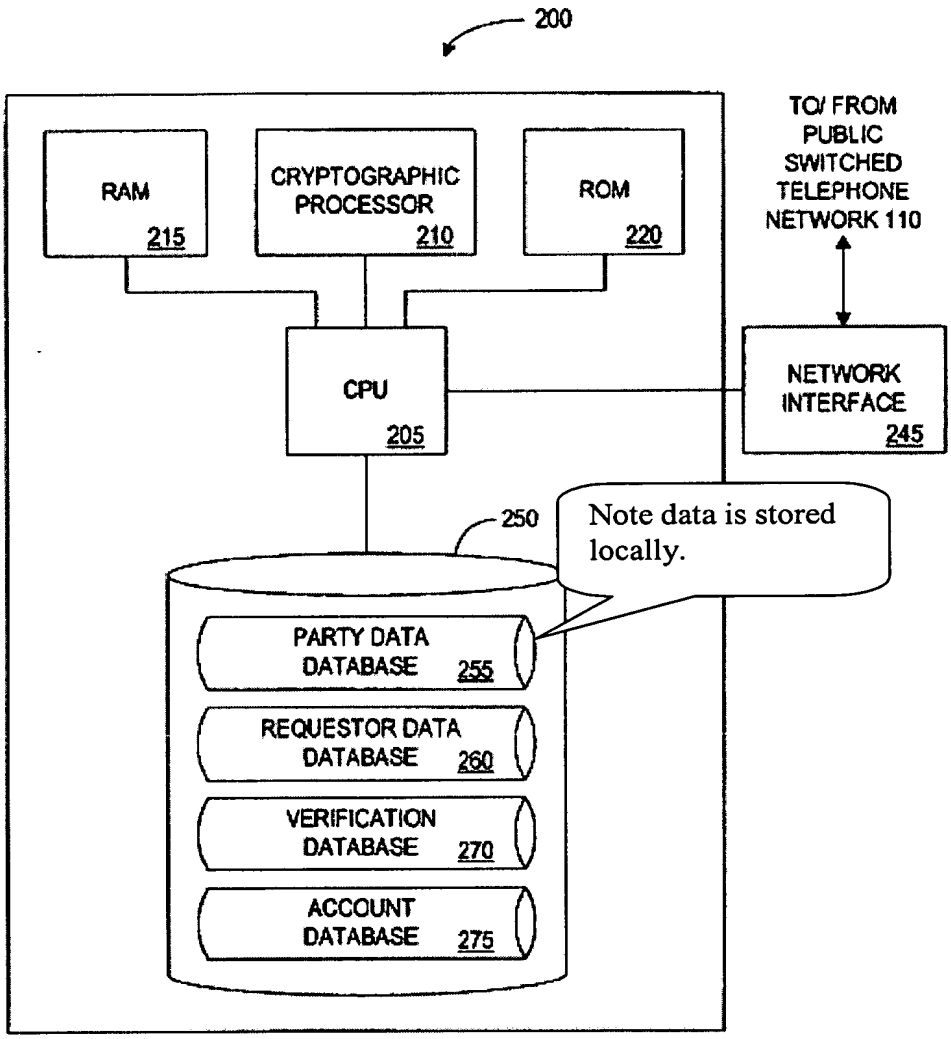
See *Walker* Fig. 1 below:




The Walker Abstract explains: "A system for facilitating employment searches using anonymous communications includes a plurality of party terminals, a plurality of requestor terminals, and a central controller. The system receives and stores employment data about prospective employment candidates. Upon receiving criteria for candidates of interest from an employer and authorization from the candidates, the central controller releases to the employer the employment data associated with the candidates. The system also establishes

communications channels between the employer and the candidates, while maintaining their anonymity."

According to Walker, both the user (job seeker) personal data and the employer (requestor) data are stored in local database, fully accessible to the central controller. This is illustrated in Walker's Fig. 2A reproduced below (bubble caption added):




Thus *Walker* discloses how to use the release of confidential or sensitive information as a method for establishing anonymous communications. It can run employer search criteria against the "party database" to find suitable candidates for employment. See Walker Fig. 2B. Walker can list data that "has been verified" (See Fig. 2C), but it does not teach how to effectively verify or authenticate a subject's identity as in the present invention. That is not its purpose or intent.

Rather, Walker et al. state that, "A goal of the invention is to provide a communication system incorporating a central database of information supplied by one or more parties and managed by a central administrator where all parties to the system can manage and control the release of any or all information about themselves or their identities, and where such a system allows for electronic-based communications between the parties without the necessity of revealing the identity of either party." [Emphasis added.]

The system of Claim 1, by contrast, does not require a central database (whether or not managed by a central administrator), but rather pertains to making independently operated databases, controlled by different entities (*their* respective owners or proprietors), appear as a single database for the specific purpose of making querying across multiple databases easy. For example, note that Claim 1 includes:

> "multiple independently operated databases, each database storing information associated with the subject, the associated information being accessible only through predefined queries to identify the subject; and
>
> "a verification engine for facilitating authentication of the subject by receiving the authentication request, selecting one or more of the predefined queries, presenting the one or more selected queries to the subject via the authenticating client, receiving from the subject an answer to each of the one or more selected queries, and presenting the answer to the multiple independently operated databases for a validation response."

This system is not disclosed by *Walker*. Similar arguments may be made with respect to the system of Claim 4 and the method of Claim 5.

As another example, new Claim 6 calls for, in pertinent part:

> "providing a database interface for interacting with an independent, remote, third-party database without storing any significant portion of the third-party database locally, and wherein the interaction is limited to submitting a query among a predetermined set of permitted types of queries, and receiving from the third-party database a response to the permitted query..."

Thus the remote third-party database is protected from disclosure or copying, yet it can be leveraged effectively to provide effective, efficient authentication of a subject's identity. As noted in the present specification: [0029] "On the back end, the system also has tight controls for the questions it asks of each database. This enables it to meet the stringent privacy requirements of many database holders. The ability to control the types of queries being made against the database provides many database providers the incentive, or at least

comfort level to make their database available to the verification engine. The independent database operator can authorize a query to access whatever level of information they are comfortable with. This makes available the use of their information in legitimate ways that were not previously possible."

Thus, in accordance with the system of Claim 6, it is very specifically not true that "all parties to the system can manage and control the release of any or all information about themselves or their identities". On the contrary, only the owners (licensees or other proprietors are considered "owners" for present purposes) of each associated database can control the release of information from their database, and that information has nothing to do with their own identities. It has to do with information associated with the identity of the person seeking authentication, and that person very specifically does not have the right to control release of information within the system. The system requires the existence of information not controlled or assembled by the person whose authentication is being sought. This is exactly the opposite of Walker.

For these reasons, the pending claims clearly distinguish over *Walker* and should be allowed.

Respectfully submitted,

By _____
John A. Rafter, Jr.
Registration No. 31,653 for
Micah D. Stolowitz
Registration No. 32,758

STOEL RIVES LLP
900 SW Fifth Avenue, Suite 2600
Portland, OR 97204-1268
Telephone: (503) 224-3380
Facsimile: (503) 220-2480
Attorney Docket No. 29094/14:2